

From:

Jay Liu
Product Manager
TP-Link Technologies (SG) Pte. Ltd.
12 Kallang Avenue #03-30 Aperia
Singapore 339511
Jay.liu@tp-link.com
+65 85800775

Views from TP-Link on “IMDA TS RG-SEC”

To:

Aileen Chia (Ms)
Deputy Chief Executive (Policy, Regulation & Competition Development)
Director-General (Telecoms & Post)
Infocomm Media Development Authority
10 Pasir Panjang Road
#03-01 Mapletree Business City
Singapore 117438

We have our views on following requirements:

1. 4.1.2.a&b

Original Requirements:

- a. The minimum length of a password shall be 10, and shall meet at least 3 out of the following 4 complexity rules:
 - i. Minimally 1 uppercase character (A-Z)
 - ii. Minimally 1 lowercase character (a-z)
 - iii. Minimally 1 digit (0-9)
 - iv. Minimally 1 special character (punctuation and/or space)
- b. The password shall not have consecutive identical characters.

TP-Link's View:

Our Concern is these 4 rules make the password too complicated that end user will easily **forget**. For RG normally end user will only use the password when the first time they did the set up, then they will not use the password for 1-2 years. If the password is too complicated, the user will forget and make the significant lower user experience in this part.

We suggest to balance between the password strength and user experience:

- (a. The minimum length of a password shall be **6**, and shall meet at least **2** out of the following 4 complexity rules:
 - i. Minimally 1 uppercase character (A-Z)
 - ii. Minimally 1 lowercase character (a-z)

- iii. Minimally 1 digit (0-9)
- iv. Minimally 1 special character (punctuation and/or space)

2. 4.2.1.a

Original Requirements:

- a. Residential Gateway shall turn off the following system services by default:
 - i. WPS
 - ii. HNAP

TP-Link's View:

There are two WPS methods:

one is to connect router by inputting Router's Pin, the other is by pushing WPS button. For TP-link's devices, the former method has security mechanism to protect against brute force, and will be disabled when input error pin more three times.

The latter is a useful method for quick connection if the user has device on hand, **so we suggest turning on WPS by default.**

3. 4.2.2

Original Requirements:

- First attempt to access to admin page/settings should be conducted through wired connection.
- If wireless connection is used, the wireless communication should leverage at least AES encryption, with at least WPA2 protection.

TP-Link's View:

For **compatibility reasons**, the default mode is auto/auto rather than WPA2-AES.

4. 4.2.3.d&e

Original Requirements:

- d. Login account shall be blocked after a fixed number of unsuccessful login attempts.
- e. Secure alternative authentication mechanism shall be provided to fall-back on, when a login account is blocked. ([GSMA CLP.13])

TP-Link's View:

the account will be blocked for 20 mins, our thinking please kindly see below.

same concern as 4.1.2a. Normally end user will not use the login/password frequently which let people easily forget the password.

Also people will forget the alternative authentication info.

Normally end user will reset the RG and do the set up again.

We do not think the alternative authentication mechanism will either improve the security or user experience.

5. 4.3.e

Original Requirements:

e. Minimum period of the firmware support received by the Residential Gateway shall be provided upfront to the user.

TP-Link's View:

We do not understand this requirement, please help to clarify what it means.

6. 4.4.a

Original Requirements:

a. Residential Gateway should employ strong password as described in Section 4.1.2 for Wi-Fi connection.

TP-Link's View:

Same concern as 4.1.2a.